Konferencja prasowa

„Światowy Dzień konsumenta – bezpieczne zakupy i aukcje internetowe”

Warszawa, 15 marca 2006

Zawartość:

- Największe zagrożenia dla konsumentów w Internecie
- Jak bezpiecznie kupować w sklepach internetowych?
- Jak bezpiecznie kupować na aukcjach internetowych?
- Uprawnienia konsumenta przed niechcianą korespondencją elektroniczną
- W jaki sposób konsument może się chronić od strony technicznej przed internetowymi oszustwami?
- Ochrona dzieci przed zagrożeniami w Internecie
- Internetowi naciągacze…
- Przestępstwa komputerowe (cyberprzestępczość)
- Na co uważać w umowach z dostawcami usług internetowych?
- Słowniczek

NAJWIĘKSZE ZAGROŻENIA DLA KONSUMENTÓW W SIECI

Internet jest obecnie najszybciej rozwijającym się medium zapewniającym praktycznie nieograniczone możliwości komunikacji i ludzkiej aktywności na całym świecie. Wirtualny świat tworzony przez sieć nie jest jednak pozbawiony zagrożeń, częstokroć nieróżniących się niczym od tych, które można spotkać w realnym świecie. Główne obszary wzmożonej uwagi konsumenta powinny koncentrować się wokół:

- zapewnienia możliwie najwyższego poziomu jasnej, pełnej i precyzyjnej informacji (głównie podczas dokonywania zakupów w sieci),
- zapewnienia jak największego poziomu bezpieczeństwa przy korzystaniu z usług internetowych (problem cyberprzestępczości),
- dynamiki rozwoju Internetu, a co za tym idzie pojawiających się coraz nowych typów zagrożeń oraz oszustw – a także elastycznego reagowania na nie,
- edukacji konsumenta w zakresie uprawnień, jakie posiada w wirtualnym świecie.

JAK BEZPIECZNIE KUPOWAĆ W SKLEPACH INTERNETOWYCH ?

Coraz częściej dokonujemy zakupów siedząc w domu przed komputerem. Choć to bardzo wygodna forma robienia zakupów, musimy pamiętać o tym, że nie wszystkie sklepy internetowe zachowują się fair wobec klientów. Najczęściej spotykane naruszenia przepisów prawa to: brak pełnych informacji o firmie, produktach, kosztach zakupów, brak jasnego opisu towaru, niewyraźne, czasami bardzo małe zdjęcia, zbyt długie dostarczanie produktów, ukrywanie możliwości zwrotu towarów. Konsument nie pozostaje jednak bezbronny, gdyż posiada kilka specyficznych uprawnień wynikających z umów w handlu elektronicznym.

Czy przedsiębiorca może zawrzeć umowę z wykorzystaniem poczty elektronicznej bez zgody konsumenta?

Posłużenie się środkiem komunikacji elektronicznej w celu złożenia propozycji zawarcia umowy może nastąpić wyłącznie za wcześniejszą zgodą konsumenta. Jeżeli przedsiębiorca składa propozycję zawarcia umowy na odległość, a następnie nie czekając na odpowiedź konsumenta (zamówienie), spełnia świadczenie, to zawsze działa na własne ryzyko.

Nawet, jeżeli w ramach poprzednio zawartych umów konsument przyjmował niezamówiony towar i uiszczał cenę, przy każdej następnej transakcji nie będzie do tego zobowiązany, a koszty oraz ryzyko utraty, uszkodzenia lub ubytku towaru w całości poniesie przedsiębiorca.

Jakie informacje powinien otrzymać konsument i w jakiej formie?

Najpóźniej w chwili złożenia mu propozycji zawarcia umowy, konsument powinien być poinformowany przede wszystkim o:

- imieniu i nazwisku (nazwie), adresie zamieszkania (siedziby) przedsiębiorcy,
- właściwościach oferowanych towarów,
- cenie lub wynagrodzeniu obejmujących wszystkie ich składniki, a w szczególności cła i podatki,
- zasadach zapłaty ceny lub wynagrodzenia,
- kosztach oraz terminie i sposobie dostawy,
- prawie odstąpienia od umowy w terminie dziesięciu dni,
- miejscu i sposobie składania reklamacji.

Wymienione informacje sklep internetowy powinien także potwierdzić na piśmie.

W jakich sytuacjach prawa konsumenta są ograniczone?

Nie zawsze zawierając umowę on-line można korzystać z pełni praw konsumenckich. Istnieją pewne, ściśle wyszczególnione ograniczenia. Niektóre uregulowania, dotyczące np. prawa odstąpienia od umowy, nie znajdują zastosowania w przypadku: sprzedaży artykułów spożywczych dostarczanych okresowo przez sprzedawcę do mieszkania lub miejsca pracy konsumenta, świadczenia usług turystyczno-wypoczynkowych (tj. zakwaterowania, transportu, rozrywek, gastronomii), sprzedaży z licytacji.

Gdy ochłoniesz…

Z zakupu dokonanego w sklepie internetowym można zrezygnować w ciągu 10 dni bez podawania przyczyn. Termin ten obowiązuje przy dokonywaniu zakupów w polskich sklepach internetowych (dla przykładu można wskazać, że w Wielkiej Brytanii czy Francji termin wynosi tylko 7 dni, podczas gdy w Niemczech, Szwecji są to dwa tygodnie). Termin ten biegnie od daty dostarczenia zakupionych towarów, a w przypadku usługi od dnia zawarcia umowy. Do zachowania terminu wystarczy wysłanie

oświadczenia przed jego upływem. Może on ulec wydłużeniu do trzech miesięcy jeżeli sprzedawca nie poinformował konsumenta o tym prawie.

Należy jednak pamiętać, że prawo odstąpienia od umowy zawartej na odległość nie przysługuje konsumentowi w wypadkach:

- świadczenia rozpoczętego, za zgodą konsumenta, przed upływem terminu na zastanowienie się,
- nagrań audialnych i wizualnych oraz zapisanych na nośnikach programów komputerowych po usunięciu przez konsumenta ich oryginalnego opakowania (kasety video i audio, CD, DVD i inne),
- świadczeń o właściwościach określonych przez konsumenta w złożonym przez niego zamówieniu lub ściśle związanych z jego osobą,
- świadczeń, które z uwagi na ich charakter nie mogą zostać zwrócone lub których przedmiot ulega szybkiemu zepsuciu,
- dostarczania prasy.

W przypadku rezygnacji z zakupu, umowa między konsumentem a sprzedawcą uznawana jest za niezawartą, a obie strony zwolnione są ze wszelkich zobowiązań. Towar powinien zostać zwrócony w stanie niezmienionym (czyli nieużywanym). Za wyjątkiem wskazanych powyżej produktów można dokonać zwrotu towaru po usunięciu oryginalnego opakowania. Ponadto należy podkreślić, że sklep internetowy nie może żądać od konsumenta zapłaty za wycofanie się z umowy (odstępnego) – takie żądanie jest bezprawne i nawet jeśli zostało zapisane w umowie, jest nieważne.

Najważniejsze obowiązki sklepów internetowych

- obowiązek jasnego poinformowania konsumentów o prawie odstąpienia od umowy; prawo to nie może być uzależniane od zapłaty przez konsumenta jakiegokolwiek odstępnego,
- obowiązek zapewnienia jasnej i pełnej informacji o oferowanych towarach i usługach,
- obowiązek czytelnego poinformowania konsumenta przed transakcją o swoich danych teleadresowych,
- obowiązek podawania pełnej ceny oferowanych towarów – już po doliczeniu wszelkich podatków i ewentualnych ceł,
- obowiązek informowania o pełnych kosztach, terminie i sposobie dostawy,
- obowiązek dokładnego opisania procedury reklamacyjnej i jej warunki,
- obowiązek pisemnego potwierdzenia informacji o dokonaniu zakupu.

Najczęstsze naruszenia przepisów prawa przez sklepy internetowe

- brak pełnych informacji o firmie, produktach, kosztach zakupów, brak jasnego i precyzyjnego opisu towarów,
- zbyt długie dostarczanie produktu lub usługi,

  Komentarz: Jeżeli nie umówiliśmy się ze sprzedawcą inaczej, powinien on zrealizować umowę najpóźniej w ciągu 30 dni po jej zawarciu. Oznacza to, iż w umowie ze sprzedawcą internetowym może znajdować się krótszy lub dłuższy (np. 15 lub 45 dni) termin realizacji zamówienia. Jeżeli przedsiębiorca nie może spełnić świadczenia powinien niezwłocznie, nie później jednak niż do 30 dni od zawarcia umowy, zawiadomić o tym konsumenta i zwrócić cała otrzymaną od niego kwotę.

- brak informacji o możliwości zwrotu towarów i prawie odstąpienia od umowy,

  Komentarz: zdarza się, że sklepy internetowe nie informują swoich klientów, że mogą zwrócić zakupiony towar w terminie 10 dni – podczas gdy taką możliwość dają przepisy prawa dotyczące sprzedaży na odległość. Tymczasem, jasna i czytelna informacja o możliwości zwrotu towaru jest doskonałym chwytem marketingowym i na pewno rozwiałaby wiele obaw związanych z zakupami.

Porady dla konsumenta dokonującego zakupów w sklepach internetowych

- Poznaj sprzedawcę! (wiem gdzie znajduje się siedziba sklepu i jak skontaktować się ze sprzedawcą)

Upewnij się, że posiadasz nie tylko adres poczty elektronicznej sprzedawcy, ale też adres pocztowy i numer telefonu – to na wypadek konieczności kontaktu ze sprzedawcą, gdy nabyty towar lub usługa okazały się wadliwe, niezgodne z umową. Wybieraj sklepy internetowe o ugruntowanej renomie lub rekomendowane przez osoby zaufane, pisma fachowe itp.

- Wiesz, co kupujesz! (sklep internetowy zapewnił mi pełny oraz precyzyjny opis towaru i dokładnie się z nim zapoznałem)

Upewnij się, że wiesz, co kupujesz. Przeanalizuj dokładnie wszystkie informacje o produkcie, schematy, zdjęcia, wymiary, itp. Zastanów się, czy rozumiesz, jak działa produkt lub usługa, którą chcesz nabyć. W razie potrzeby lub jakichkolwiek wątpliwości poproś sprzedającego o dokładniejsze i pełniejsze informacje.

- Sprawdź cenę! (znam całkowity koszt zakupu, łącznie z podatkiem, cłem, transportem)

Cena, którą zapłacisz powinna być precyzyjnie określona. Nie zapominaj o dodatkowych kosztach jak np. ubezpieczenia, cła, podatki, opłaty za pakowanie, itp. Zwróć uwagę, jakie są koszty przesyłki.

- Uważaj jak płacisz! (wiem, że sklep gwarantuje mi bezpieczny sposób zapłaty)

Zawsze sprawdź, jakie są możliwości zapłaty. Bądź zawsze ostrożny podając numer karty przez Internet. Zawsze sprawdź, czy znajdujesz się na bezpiecznej stronie internetowej, zanim podasz swoje dane on-line (bezpieczne połączenie https://, ikonka kłódki). Pamiętaj o potwierdzeniu zamówienia zanim zapłacisz.

- Sprawdź szczegóły dotyczące doręczenia przesyłki i warunki ewentualnego odwołania zamówienia! (sklep internetowy poinformował mnie dokładnie o terminie zapewnienia dostępności produktu oraz terminie jego dostawy)

Jeśli sprzedawca nie będzie w stanie zagwarantować terminu dostarczenia przesyłki, może lepiej zrezygnować z zakupu. Pamiętaj o prawie odstąpienia od umowy w terminie 10 dni od wydania rzeczy. Aby zrezygnować ze zrealizowanego już zamówienia nie musisz podawać konkretnego powodu. Jeśli powiadomisz sprzedawcę, na piśmie lub za pomocą poczty elektronicznej, że chcesz zwrócić zakupiony towar, sprzedawca zobowiązany jest uwzględnić Twoje życzenie. Wyjątek stanowią tu m.in. żywność, rozpakowane płyty CD, kasety video i oprogramowanie komputerowe.

- Czy to jest na gwarancji?! (sklep internetowy poinformował mnie, jak i kiedy mogę zwrócić towar)

Upewnij się, czy sprzedawca zapewnia gwarancję, bądź serwis produktu lub usługi, którą kupujesz. Sprawdź, co sprzedający gwarantuje, a czego nie i jak długo trwa okres gwarancyjny. Pamiętaj, że masz 2 lata na reklamowanie niezgodności towaru z umową. Jeżeli wadliwy produkt nie może być naprawiony lub wymieniony, masz prawo do zwrotu części lub całej kwoty, jaką zapłaciłeś.

- Zachowaj rachunki i inne informacje dotyczące zamówienia!

Zachowaj wszystkie rachunki i inne dokumenty, które otrzymałeś podczas dokonywania zakupu. Wydrukuj lub skopiuj zamówienie, jeśli kupujesz on-line lub za zamówieniem pocztowym. To samo dotyczy zasad i warunków zakupu, które przedstawione były na stronie internetowej (kopię strony internetowej możesz wykonać wykorzystując klawisz „PrintScrn"). Zatrzymaj katalog sprzedawcy i całą korespondencję ze sprzedającym, gdyż może okazać się bardzo potrzebna w razie pojawienia się problemu.

- Zabezpieczaj i chroń swoje dane!

Dane personalne mogą być wykorzystywane jedynie za Twoją zgodą. Kwestionariusze do składania zamówienia, do których wpisujesz swoje dane, powinny zawierać pytanie, czy zgadzasz się na przetwarzanie danych osobowych celem realizowania zamówienia. Jeżeli na formularzu nie ma pytania dotyczącego zgody na przetwarzanie danych osobowych, zapytaj sprzedawcę, w jaki sposób firma realizuje politykę prywatności i ochrony danych osobowych.

- Pamiętaj, że jeżeli coś wydaje się zbyt atrakcyjne, aby było prawdziwe, najprawdopodobniej tak właśnie jest!

JAK BEZPIECZNIE KUPOWAĆ NA AUKCJACH INTERNETOWYCH?

Internetowe aukcje to strony internetowe, które pozwalają sprzedawać różnego rodzaju towary poprzez licytację. Ta forma zakupów w sieci staje się coraz bardziej popularna jednak należy uważać na istotne problemy, jakie się z nią wiążą. Przede wszystkim nie można zapominać, że co do zasady nie kupujemy ze strony aukcyjnej jako takiej, toteż taka strona nie będzie ponosiła odpowiedzialności gdy pojawią się problemy z nabytym towarem. Pozyskajmy dane kontaktowe sprzedawcy i skontaktujmy się z nim niezależnie od organizatora aukcji internetowej aby sprawdzić, czy on rzeczywiście w niej uczestniczy. Pomocne mogą być komentarze i opinie dotyczące sprzedawcy pojawiające się na forum organizatora aukcji (forum dyskusyjne, chat-room, itd.)

Najczęściej zadawane pytania (FAQ):

- Czy mogę w terminie 10 dni odstąpić od umowy zawartej na aukcji internetowej?

Przy sprzedaży z licytacji konsumentowi nie przysługuje prawo do odstąpienia od umowy w terminie 10 dni. Odstąpienie od umowy będzie możliwe tylko wtedy, gdy konsument dokonał zakupu na aukcji internetowej od przedsiębiorcy bez licytacji po ustalonej z góry cenie, np. w opcji „kup teraz". W tej sytuacji prawo konsumenta to odstąpienia od umowy nie przysługuje tylko w przypadku zakupu: dostarczania prasy, nagrań audialnych i wizualnych oraz zapisanych na nośnikach programów komputerowych po usunięciu przez konsumenta ich oryginalnego opakowania, świadczeń o właściwościach określonych przez konsumenta w złożonym przez niego zamówieniu lub ściśle związanych z jego osobą, świadczeń, które z uwagi na swój charakter nie mogą zostać zwrócone lub których przedmiot ulega szybkiemu zepsuciu.

- **Jak działają firmy depozytowe (escrow companies)?**

Firm depozytowe funkcjonują jako pośrednicy w sprzedażach internetowych wg schematu: kupujący wysyła im zapłatę, sprzedawca wysyła im towar i kiedy otrzymają zarówno zapłatę jak i towar przekazują świadczenia dalej – tzn. nabywca otrzymuje towar a sprzedawca pieniądze. Dla własnego dobra należy korzystać tylko z usług firm polecanych przez organizatora aukcji na jego stronie.

- **W jaki sposób mogę sprawdzić paczkę z towarem zakupionym na aukcji internetowej?**

Poczta Polska oferuje specjalną usługę, dzięki której przed zapłaceniem za przesyłkę można sprawdzić, czy znajduje się w niej towar, który zamówiliśmy w sieci. Żeby skorzystać z usługi, należy

zamawiając towar zaznaczyć, że chcemy, aby nadawca zapłacił dodatkowo 5 złotych i zamówił usługę „sprawdzenie zawartości przesyłki przez odbiorcę".

Wskazówki dla dokonywania bezpiecznych zakupów na aukcjach internetowych:

- Pamiętajmy, że co do zasady nie kupujemy ze strony aukcyjnej jako takiej, toteż taka strona nie będzie ponosiła odpowiedzialności gdy pojawią się problemy z nabytym dobrem.

  Komentarz: Operator serwisu aukcyjnego nie jest stroną umowy sprzedaży, którą zawierają między sobą tylko jego użytkownicy. To oznacza, że operator nie może ponosić odpowiedzialności za wykonanie tej umowy, czyli za dostarczenie kupującemu właściwego towaru lub za jego wady. Odpowiedzialny z tego tytułu jest wyłącznie sprzedawca.

  Operator serwisu może natomiast ponosić ewentualnie odpowiedzialność odszkodowawczą względem oszukanych osób z tytułu nienależytego świadczenia usługi dostępu do serwisu aukcyjnego.

- Zadbajmy o właściwe zabezpieczenie danych dotyczących naszego konta w serwisie aukcyjnym. Zainstalujmy i aktualizujmy program antyszpiegowski i antywirusowy. Uniemożliwi to przejęcie naszego konta przez inną osobę.

- Chrońmy swoje konto nie tworząc zbyt prostych haseł. Jeśli korzystamy z kawiarenki internetowej, pamiętajmy o wylogowaniu się z serwisu.

- Dokładnie zapoznajmy się z opisem przedmiotu kupowanego na aukcji i warunkami sprzedaży. W razie wątpliwości pytajmy sprzedającego.

- Unikajmy zawierania transakcji z osobami, które wysyłają towar **tylko** po uprzednim przelaniu pieniędzy na podany rachunek.

- Pozyskajmy dane kontaktowe sprzedawcy i skontaktujmy się z nim jeszcze przed licytacją aby wyjaśnić szczegóły transakcji: sposób zapłaty, koszty transportu, sposób wysłania przedmiotu, jego opakowanie, ewentualne ubezpieczenie.

- Jeżeli sprzedawca jest z naszej miejscowości, starajmy umawiać się na osobisty odbiór towaru.

- Czytajmy komentarze i świadectwa o danym sprzedawcy, ewentualnie opinie pojawiające się na forum wewnętrznym w witrynie internetowej organizatora aukcji (forum dyskusyjne, chat-room, itd.). Pamiętajmy, że większość opinii, które pojawiają się dzień lub dwa po zakończeniu transakcji, są wątpliwej wiarygodności. Przesyłka towaru zwykle trwa dłużej. Ponadto, duża liczba pozytywnych komentarzy to jeszcze nie wszystko. Sprawdzajmy za co zostały wystawione. Jeśli wcześniej sprzedawca oferował tylko tanie produkty i nie ma komentarzy za

transakcje dotyczące drogiego towaru, to istnieje ryzyko trafienia na oszusta. Zwracajmy uwagę na to czy komentarze na koncie sprzedającego wystawiane są przez różne osoby.

- Nigdy nie opuszczajmy specjalnego połączenia w celu dopełnienia czynności związanych z zakupem poza aukcją, gdyż wtedy nie będziemy chronieni przez organizatora aukcji.
- Do zapłaty korzystajmy z systemów bezpiecznej płatności albo polecanych przez organizatora aukcji serwisów pośredniczących. Kupujący płaci wówczas nie bezpośrednio sprzedawcy, tylko przekazuje pieniądze serwisowi. A ten wypłaca je dopiero wtedy, gdy otrzyma od kupującego informację, że dostał towar i jest on zgodny z umową.
- Nie ufajmy sprzedawcom, którzy zobowiązują się opłacić koszt przesyłki. W obrocie aukcyjnym przyjmuje się, że za przesyłkę płaci kupujący.
- Korzystajmy z serwisów aukcyjnych, które oferują różnego rodzaju systemy ochrony kupujących. Polegają one zwykle na zapewnieniu kupującemu zwrot wpłaconej kwoty (do górnej granicy określonej przez serwis aukcyjny) w przypadku, gdy zapłacił za towar, ale nigdy go nie otrzymał. Dotyczy to także sytuacji, kiedy kupujący otrzymał towar, znacznie różniący się od tego, który był opisany na stronie internetowej. Najważniejszym z warunków otrzymania zwrotu jest zwykle zgłoszenie sprawy na policję.
- Wykorzystujmy przesyłki z zadeklarowaną wartością i ubezpieczenie przesyłek.
- Gromadźmy korespondencję wymienianą z kontrahentem (e-maile, skany strony www), gdyż mogą okazać się przydatne w razie sporu.
- I na koniec: oszuści internetowi są tylko tak sprytni, jak my jesteśmy naiwni! Ale przestępców można pokonać!

Co zrobić, gdy zostałeś oszukany:

1) Jeżeli doszło do oszustwa, przygotuj dokumentację potrzebną na policji – np. potwierdzenie dokonania zapłaty za towar, korespondencję z kontrahentem, dane kontaktowe portalu aukcyjnego.
2) Zgłoś się na policję. Policja lub prokuratura powinna zakończyć czynności sprawdzające w ciągu 30 dni postanowieniem o wszczęciu albo odmowie wszczęcia śledztwa lub dochodzenia.
3) Jeżeli transakcja była ubezpieczona, złóż wniosek do serwisu aukcyjnego o zwrot pieniędzy.
4) Jeżeli transakcja nie była ubezpieczona, można dochodzić zwrotu pieniędzy od oszusta w procesie karnym lub cywilnym.

UPRAWNIENIA KONSUMENTA PRZED NIECHCIANĄ KORESPONDENCJĄ ELEKTRONICZNĄ

Każdego dnia nasze skrzynki e-mailowe zapełniają się stosem niechcianej korespondencji elektronicznej. Czy możemy coś z tym zrobić? Czy powinniśmy kogoś o tym informować? Czy może być to niebezpieczne?

Ochrona przed spamem

Niechciana wielokrotnie wysyłana korespondencja zarówno handlowa, czyli reklamy i oferty, jak również niemająca charakteru marketingowego, określana jest ogólnie pojęciem „spam".

Słowo *spam* pochodzi z języka angielskiego i oznacza w dosłownym tłumaczeniu konserwę mięsną (mielonkę) i jest używane dla określenia wysyłanej wielokrotnie niechcianej korespondencji, zazwyczaj w celu marketingu produktów i usług o komercyjnym przeznaczeniu. Aby zaklasyfikować daną wiadomość jako spam musi ona spełniać łącznie kilka warunków:

- jej treść nie może być uzależniona od naszej tożsamości, czyli jest to jakiś e-mail, który może być przesłany do wielu niezależnych odbiorców,
- jest to wiadomość przez nas nieoczekiwana i na której otrzymanie wcześniej nie wyraziliśmy świadomej, wyraźniej i możliwej do odwołania zgody,
- z okoliczności musi wynikać, że wysyłający odniósł z faktu wysłania tego e-maila większą korzyść, niż my z jego odbioru.

Jeżeli dana wiadomość będzie spełniała powyższe warunki, to będzie można ją zaklasyfikować jako spam. Jeżeli będzie miała ponadto charakter informacji handlowej, to zgodnie z przepisami ustawy o świadczeniu usług drogą elektroniczną, wysłanie takiej wiadomości będzie stanowiło wykroczenie i będzie zagrożone karą grzywny w wysokości od 20 zł do nawet 5000 zł.

Informacją handlową jest każda informacja przeznaczona bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku przedsiębiorcy lub osoby wykonującej zawód. Ponadto informacja handlowa powinna zostać wyraźnie wyodrębniona i oznaczona w sposób niebudzący wątpliwości, że jest informacją handlową. Przesyłka taka wymaga zgody usługobiorcy, przy czym nie może być ona domniemana ani dorozumiana z oświadczenia woli o innej treści.

W sytuacji otrzymania spamu przede wszystkim należy upewnić się, czy nie wyraziliśmy zgody na otrzymywanie korespondencji od nadawcy. Jeżeli informacja o udzieleniu zgody znajduje się w otrzymanym liście i jest ona prawdziwa, mamy prawo w każdej chwili, bez podawania przyczyny, zgodę tę odwołać**.** Wystarczy przesłać pocztą elektroniczną następującą treść: „Sprzeciwiam się

dalszemu wykorzystywaniu przez Waszą firmę moich danych osobowych do celów marketingowych i przekazywania tych danych innym podmiotom".

W tym miejscu należy przypomnieć, że przy zakładaniu darmowych kont internetowych na popularnych portalach warunkiem koniecznym do dokonania pełnej rejestracji jest wyrażenie zgody na otrzymywanie określonego rodzaju informacji handlowych. W związku z tym dopuszczalne jest wysyłanie komunikatów handlowych na takie konto.

Jeżeli list został wysłany bez naszej zgody, w żadnym wypadku nie należy na niego odpowiadać. Odpowiedź będzie dla spamera sygnałem, że jego list rzeczywiście dotarł i poznaliśmy jego treść. To upewni go, że adres działa i warto na niego wysyłać kolejne oferty. Ta sama zasada dotyczy możliwości wypisania się z list dystrybucyjnych przez kliknięcie odnośnika w liście (np. dostajesz informację handlową z dopiskiem: „Jeżeli nie zgadzasz się na otrzymywanie następnych wiadomości, odpisz na adres „xxx@spam.com.pl") – zazwyczaj zamiast pożądanego skutku, zaowocuje to większą ilością niechcianej korespondencji.

Jeżeli uważasz, że Twoje dane osobowe są wykorzystywane bezprawnie lub gdy otrzymujesz niezamówione informacje handlowe, możesz:

- złożyć zawiadomienie na policję w związku z popełnieniem wykroczenia

lub

- złożyć skargę do:

- Urzędu Ochrony Konkurencji i Konsumentów (www.uokik.gov.pl),
- Federacji Konsumentów (www.federacja-konsumentow.org.pl),
- Powiatowego (Miejskiego) Rzecznika Konsumentów,
- Generalnego Inspektora Ochrony Danych Osobowych (www.giodo.gov.pl).

Dla naszej wygody, w najbliższym czasie zostaną również uruchomione specjalne skrzynki pocztowe w różnych organach administracji, do których będziemy mogli zgłaszać spamy. Tzw. „spamboxy" zostaną uruchomione w Ministerstwie Transportu i Budownictwa (MTiB), u Generalnego Inspektora Ochrony Danych Osobowych (GIODO), w Urzędzie Ochrony Konkurencji i Konsumentów (UOKiK) oraz w Urzędzie Komunikacji Elektronicznej (UKE).

Należy również pamiętać, że spam zaczyna coraz częściej być wykorzystywany jako nośnik niebezpiecznych treści w Internecie, takich jak: wirusy, konie trojańskie, dialery i inne robaki komputerowe, które mogą instalować się na naszych komputerach, niszczyć zawartość dysków, szpiegować nasze zachowania w Internecie albo przekierować nasze połączenia na numery

o podwyższonej płatności. Dlatego pod żadnym pozorem nie należy otwierać załączników do wiadomości od nieznanych nadawców albo takich, których się nie spodziewamy.

Przypadki zagrożenia lub naruszenia bezpieczeństwa w sieci Internet możesz też zgłosić do zespołu CERT Polska (www.cert.pl) lub swojego dostawcy usług, ale pamiętaj o tym, że sama treść wiadomości wyświetlana przez program pocztowy nie wystarcza do ustalenia rzeczywistego źródła listu. W szczególności wszystkie informacje zawarte w polu „Od" i „Do", a więc dane nadawcy i odbiorcy, mogą być sfałszowane przez nieuczciwego wysyłającego. Dlatego nigdy pochopnie nie wysyłaj skarg na nadawcę, opierając się jedynie na tych informacjach. Przy przekazywaniu wiadomości w celu zbadania jej przez eksperta, załącz pełne nagłówki lub skorzystaj z opcji przesłania wiadomości jako załącznik, jeżeli Twój program ją oferuje.

W jaki sposób najczęściej trafia do nas spam?

Spam jest dla nieuczciwego sprzedawcy jedną z najtańszych form dotarcia do konsumentów ze swoją ofertą, gdyż większość kosztów przerzucona jest na odbiorcę. Ponieważ nadawcy spamu nie muszą kierować listów do określonej grupy odbiorców, którzy mogą być zainteresowani ofertą, w konsekwencji, każdy adres e-mail jest dla nich równie przydatny, niezależnie od drogi, jaką został pozyskany. Wyszukiwanie działających adresów e-mail i tworzenie list, które następnie sprzedawane są nieuczciwym sprzedawcom, stało się jedną z form działalności przestępców internetowych.

- Najbardziej narażone na otrzymywanie niechcianej korespondencji są adresy umieszczone na publicznie dostępnych stronach www – podanie adresu mailowego w czytelnej formie daje niemal stuprocentową pewność, że zostanie on odszukany przez programy przeszukujące zawartość sieci i umieszczony na listach dystrybucyjnych spamerów.
- Drugą grupą największego ryzyka są adresy używane na grupach dyskusyjnych. Ich przeglądanie dla programów jest równie łatwe jak w przypadku stron www i jest to źródło niemal równie popularne.
- Często, aby korzystać z serwisu www, musimy dokonać rejestracji z użyciem adresu e-mail. Dotyczy to zarówno rozmaitych forów dyskusyjnych, jak i dużych sklepów internetowych. Zazwyczaj przy rejestracji mamy możliwość zapoznania się z polityką prywatności stosowaną wobec udostępnianych danych. Choć w większości serwisów jest ona respektowana, czasem zawiera ona przyzwolenie na udostępnianie adresu innym podmiotom. Bywa także, że właściciel serwisu jest nieuczciwy i sprzedaje listy adresów swoich użytkowników.
- Adresy e-mail mogą być także odgadywane przez generowanie kolejnych ciągów znaków – najczęściej z wykorzystaniem słowników imion i popularnych wyrazów.

Są to najczęstsze, choć nie jedyne sposoby pozyskiwania adresów. Na przykład z komputera zaatakowanego przez wirus komputerowy mogą „wyciec", a w konsekwencji trafić na listy używane przez spamerów, adresy osób znajdujące się w książce adresowej.

Jak chronić adres e-mail?

- Używaj dwóch (lub więcej) adresów e-mail. Oddzielnym adresem posługuj się w korespondencji z przyjaciółmi i znajomymi, którym ufasz, a innym tam, gdzie zachodzi ryzyko, że adres trafi w niepowołane ręce (np. przy zakładaniu kont w serwisach www). Jeżeli okaże się, że na konto „publiczne" zaczynasz otrzymywać duże ilości spamu, po prostu z niego zrezygnuj i załóż nowe. W każdym przypadku wskazane jest oddzielenie konta prywatnego od służbowego, używanego w firmie, w której pracujesz, od prywatnego.
- Czytaj dokładnie politykę prywatności serwisu www, w którym zmuszony jesteś podać swój adres e-mail. Jeżeli taki dokument nie jest dostępny w żadnej formie, powinieneś potraktować serwis jako mało godny zaufania. Dotyczy to także serwisów oferujących bezpłatne konta pocztowe. Często rejestrując się w nich, wyrażamy zgodę na otrzymywanie korespondencji od firm trzecich. Takiej korespondencji nie możemy uznać za niezamawianą.
- Unikaj prostych i krótkich adresów. Choć są one wygodniejsze w stosowaniu, łatwo mogą paść ofiarą ataku słownikowego. Lepiej więc wybrać adres dłuższy, zawierający cyfry lub znaki specjalne, np. imie.nazwisko@poczta.isp.pl.

Najczęściej zadawane pytania (FAQ):

- Dostałam e-mail od nieznanej osoby, w którym jest napisane, że wygrałam 100 tys. dolarów. Aby otrzymać nagrodę powinnam przesłać na konto w RPA 100 dolarów na koszty manipulacyjne. Co powinnam zrobić?

  W przypadku każdej takiej wiadomości musimy przede wszystkim polegać na swoim zdrowym rozsądku. Jeżeli nie braliśmy udziału w żadnej loterii, czy konkursie, to nie możemy też nic wygrać. Dlatego najprawdopodobniej taka wiadomość stanowi próbę wyłudzenia od nas pieniędzy.

- Czy dopuszczalne jest przesyłanie przez sklep internetowy informacji handlowej osobom, które udostępniły adres e-mailowy w Internecie, np. na różnego rodzaju forach publicznych?

  Przesyłanie informacji handlowej takim osobom będzie dawało podstawę do zakwalifikowania tych informacji jako niezamówionych. Informację handlową uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na otrzymanie takiej informacji, w szczególności udostępnił w tym celu adres e-mail.

Udostępnienie adresu e-mail w Internecie, np. na forach publicznych, nie może być uznane jako udostępnienie adresu w celu otrzymywania jakichkolwiek informacji handlowych.

W JAKI SPOSÓB KONSUMENT MOŻE SIĘ CHRONIĆ OD STRONY TECHNICZNEJ PRZED INTERNETOWYMI OSZUSTWAMI?

Możesz utrudnić pracę hakerom i internetowym oszustom!

Użytkownicy komputerów i Internetu nie są bezbronni wobec sieciowych włamywaczy. Powinni stosować odpowiednie zabezpieczenia i dbać o ich aktualizację. Szkody można znacznie ograniczyć stosując procedury, które dziś powinien znać każdy użytkownik komputera:

(!) zabezpiecz komputer programem antywirusowym (inaczej zainstalowany na komputerze wirus może pomóc hakerowi w dotarciu do poufnych informacji, np. PIN-u i hasła konta bankowego),

(!) nie wchodź na stronę banku z linków prowadzących z innych stron,

(!) logując się na stronie internetowej banku unikaj korzystania z kawiarenki internetowej (ktoś mógł zainstalować na nich tzw. keyloggery, czyli programy podglądające to, co wpisujesz na klawiaturze). Jeśli korzystasz nie ze swojego komputera, po zakończeniu pracy wyczyść dysk z plików cookies – instalowanych na dysk przez strony www, na które wchodzisz, w przeglądarce Internet Explorer 6: narzędzia > opcje internetowe > usuń pliki cookies,

(!) nie otwieraj załączników w niechcianej poczcie,

(!) sprawdzaj programy pobrane z Internetu za pomocą programów antywirusowych,

(!) jeśli dostałeś e-maila lub sms z Twojego banku internetowego (lub innej firmy z usług której korzystasz) z prośbą o podanie poufnych danych, np. numeru konta, numeru karty kredytowej, numeru ubezpieczenia, haseł, PIN-ów, NIGDY NIE ODPOWIADAJ tylko skontaktuj się osobiście lub telefonicznie z bankiem – żądanie ze stuprocentową pewnością zostało wysłane przez złodzieja, podszywającego się pod bank,

(!) ustaw swoją przeglądarkę internetową tak, aby nie pozwalała otwieranym stronom na niekontrolowane operacje na dysku komputera:

w przeglądarce Internet Explorer 6: narzędzia > opcje internetowe > zaawansowane > zabezpieczenia i włącz:

- „nie zapisuj szyfrowanych stron na dysku”
- „ostrzegaj przed nieważnymi certyfikatami witryn”
- „ostrzegaj przy zmianie trybu zabezpieczonego na niezabezpieczony”
- „sprawdź czy certyfikat serwera nie został cofnięty”
- „użyj SSL 3.0”

w przeglądarce Internet Explorer 6: narzędzia > opcje internetowe > zaawansowane > zawartość > autouzupełnianie i wyłącz:

- „nazwy użytkowników i hasła w formularzach”,

(!) nie zapisuj numeru PIN ani haseł w plikach tekstowych na twardym dysku komputera.

Operacje finansowe w Internecie

Operacje finansowe prowadzone za pośrednictwem konta internetowego są coraz skuteczniej chronione przed włamaniami hakerów. Na razie oszukańcze transakcje to, według różnych szacunków, ułamek procentu płatności w Internecie (0,07 proc.). Jednak płatności w Internecie przybywa, a za tym wzrasta liczba oszustw. Rozwija się również e-handel. Jednym z systemów zabezpieczeń jest identyfikator, hasła i login stosowane równocześnie, a także urządzenie zwane tokenem.

Identyfikator użytkownika i hasła są informacjami wykorzystywanymi podczas logowania. Sam identyfikator użytkownika to indywidualny numer przypisywany użytkownikowi.

Dobrym sposobem zabezpieczenia się przed hakerami jest token. Jest to urządzenie wielkości małego kalkulatora generujące ciąg cyfr, które służą jako hasło do potwierdzenia operacji wykonywanych przez Internet. Co 30 sekund lub co minutę zmienia się zestaw cyfr. Sam dostęp do tokena jest chroniony numerem PIN.

Inną formą haseł jednorazowych są zdrapki lub dostarczane listy jednorazowych haseł w formie papierowej.

W praktyce wysokiego poziomu ochrony bezpieczeństwa wymagają tylko transakcje umożliwiające dokonywanie przelewów wszelkiego rodzaju oraz zleceń stałych, pobieranie pieniędzy z bankomatu itp.

Kiedy płacisz kartą kredytową w Internecie:

- nie loguj się na stronie, na której nie ma w dolnym rogu żółtej kłódki – symbolu certyfikatu bezpieczeństwa,
- przed dokonaniem płatności sprawdź, czy w adresie internetowym są litery https (jeśli ich nie ma, oznacza to, że mamy do czynienia z powszechnie dostępną, niezabezpieczoną stroną internetową),
- aktualizuj programy chroniące komputer przed atakami internetowych oszustów,
- w żadnym wypadku nie odpowiadaj na e-maile z banku zawierające prośbę o podanie numeru konta i/lub numeru karty kredytowej i/lub kodu PIN (banki nigdy nie żądają tą drogą takich informacji).

Rodzaje kart:

- karta debetowa – pozwala na dysponowanie pieniędzmi znajdującymi się na rachunku bieżącym. Nie można nią zaciągnąć kredytu ani przekroczyć salda rachunku.
- karta kredytowa – umożliwia zadłużenie się w banku do wysokości przyznanego limitu. Jest to z reguły karta wypukła (w wytłoczonym numerem, imieniem i nazwiskiem właściciela), która umożliwia dokonywanie płatności w Internecie.
- karta obciążeniowa – charge – zbliżona do karty kredytowej, z tą różnicą, że o ile w przypadku karty kredytowej o terminie spłaty zadłużenia decydujemy sami, o tyle zadłużenie w karcie obciążeniowej bank raz w miesiącu sam ściągnie z naszego konta. Kartą można płacić przez Internet.

OCHRONA DZIECI PRZED ZAGROŻENIAMI W INTERNECIE

Jak możemy chronić nasze dzieci przed negatywnym i niebezpiecznym oddziaływaniem Internetu? Podobnie jak w realnym świecie: informując, edukując i zaszczepiając odpowiedzialne zachowania. Spędzając czas z dziećmi i surfując razem, możemy zaobserwować, jak reagują podczas stykania się z mylącymi lub niebezpiecznymi treściami oraz czy używają Internetu w sposób odpowiedzialny.

Rozmawiajmy z dziećmi o wiarygodności informacji, które można znaleźć w Internecie, aby nauczyć je krytycyzmu, w tym unikania tworzenia własnych opinii na podstawie fragmentarycznej lub odgórnie podanej informacji. Przyzwyczajajmy je do krytycznego oceniania wiarygodności informacji, które znajdują w Internecie.

Filtrowanie

Istnieje szeroki wachlarz rozwiązań technicznych umożliwiających filtrowanie dostępnych danych podczas korzystania przez dzieci z Internetu. Należy jednak pamiętać, że, po pierwsze, nic nie zapewni krytycznego i ostrożnego podejścia do dostępnych treści i danych, po drugie, zdarza się, że filtry mogą zablokować zupełnie bezpieczne zawartości przy jednoczesnym braku zatrzymania treści szkodliwych.

Skuteczność filtrowania, odnosząca się do najpowszechniejszych niepożądanych treści, takich jak pornografia, wulgarność, przemoc, zależy od działania mechanizmu i możliwości personalizacji programu filtrującego.

Większość programów jest w stanie zablokować strony z treściami z listy niecenzuralnych lub obraźliwych. Można je uaktualniać przez Internet, a czasami również personalizować. Niektóre z tych programów blokują dostęp do witryn, które zawierają „podejrzane" słowa lub obrazy; inne jedynie blokują witryny, których adresy zawierają „podejrzane" słowa.

Rzeczywista zdolność filtrowania zależy również od faktu, że pewne programy można łatwo odinstalować, a zatem dziecko posiadające stosunkowo rozwinięte umiejętności korzystania z komputera może je łatwo unieszkodliwić.

Netykieta

Mimo że Internet uznawany jest za synonim wolności i otwartej przestrzeni, istnieją w nim pewne reguły zachowania, których nie należy ignorować.

Netykieta jest zespołem zasad i norm dobrych obyczajów panujących w Internecie, czyli swojego rodzaju „konstytucją" zasad dobrego wychowania użytkowników Internetu.

W związku z tym należy pamiętać, że:

- pisanie wiadomości e-mail wielkimi literami jest równoznaczne z krzykiem: unikajmy tego jeśli nie jest to całkowicie konieczne,
- wysyłanie dużych załączników (powyżej 1 Mb) może blokować lub spowalniać skrzynkę pocztową odbiorcy: lepiej przedtem go poinformować,

- wysyłanie wiadomości e-mail, takich jak „łańcuszki", jeśli nie są one wystarczająco ważne lub nie posiadają wymiaru humanitarnego, może irytować odbiorcę, jak również blokować i spowalniać system,
- wysyłanie listów-śmieci jest niedopuszczalne, jak również bardzo irytujące,
- jeśli wysyłasz tę samą wiadomość do różnych ludzi, którzy nie znają się nawzajem, należy wpisać wszystkie adresy w polu „UDW" (ukryta kopia), aby zapobiec wysyłaniu adresów każdego z odbiorców do wszystkich pozostałych.

Rady dla młodych użytkowników Internetu

- chroń dane swoje, swojej rodziny i znajomych – nie wysyłaj „internetowym" znajomym e-maili z adresem domowym, numerem telefonu, ze zdjęciem,
- podobne zasady stosuj będąc na czacie lub biorąc udział w grupach dyskusyjnych,
- pod żadnym pozorem nigdy nie wysyłaj poufnych danych, kodów, haseł,
- pamiętaj, że twój rozmówca w sieci nie zawsze jest tym, za kogo się podaje,
- jeśli w sieci spotka Cię coś nieprzyjemnego, ktoś prześle Ci obraźliwe wiadomości lub obrazy – nie odpowiadaj, i nie bój się powiedzieć o tym rodzicom lub nauczycielom,
- na spotkanie z nowopoznanym znajomym w sieci umawiaj się tylko w miejscu publicznym i nigdy nie idź na takie spotkanie sam/sama,
- nie otwieraj załączników do e-maili, które dostałeś od nieznajomych i nie klikaj na adresy stron przesłanych w takich e-mailach; to samo dotyczy ściągania programów ze stron internetowych – możesz otrzymać wirusa lub coś innego, co zniszczy dane na Twoim komputerze.

„Dyżurnet" – punkt kontaktowy do zwalczania nielegalnych treści w Internecie

W przypadku napotkania się w Internecie na strony www, na których znajdują się nielegalne treści możemy je zgłosić do punktu „Dyżurnet". W razie potwierdzenia zarzutów „Dyżurnet" przekazuje zawiadomienie do policji.

Treści, których rozpowszechnianie jest zakazane to m.in.:

- treści rasistowskie i ksenofobiczne,
- pornografia związana z prezentowaniem przemocy lub posługiwaniem się zwierzęciem,
- pornografia dziecięca (z udziałem małoletnich poniżej 15 roku życia).

Nielegalne są również strony pornograficzne nie zawierające ostrzeżenia, że prezentowane na nich treści przeznaczone są dla osób pełnoletnich.

Kontakt z „Dyżurnetem”:

- całą dobę pod numerem infolinii: 0-801-615-005
- faksem: (22) 523-10-55
- mailem: dyzurnet@hotline.org.pl
- formularz zgłoszeniowy na stronie www.dyzurnet.pl

INTERNETOWI NACIĄGACZE...

Najbardziej typowe oszustwa i triki w cyberprzestrzeni

Niemożliwe jest wskazanie wszystkich typów oszustw na jakie można się natknąć w Internecie. Do najczęściej spotykanych należą natomiast:

- **ukryte adresy** – uważaj na naciągaczy, którzy próbują sprzedawać towary lub usługi stosując anonimowe adresy poczty elektronicznej albo numery skrzynki pocztowe,
- **atak za pośrednictwem haseł –** bądź czujny gdy widzisz krzykliwe ogłoszenia w rodzaju „Jak zarobić milion!” i pamiętaj, że same hasła nie zapewniają obiecywanego rezultatu,
- **niejasne listy referencyjne, listy pochwalne –** “Tysiące usatysfakcjonowanych klientów!” – może robić wrażenie, ale rzadko otrzymasz informację, która pozwoli Ci sprawdzić wiarygodność twierdzenia,
- **obietnice natychmiastowego bogactwa** – zwykle brzmią zbyt dobrze by być prawdziwymi,
- **zapłać za ujawnienie sekretu –** czasem możesz spotkać w Internecie ofertę uzyskania sekretnej metody wzbogacenia się dla wybrańców. Tymczasem zwykle ofiarami tego wybiegu są tysiące użytkowników. Szczegóły tajemnicy są dostępne za stosowną opłatą,
- **ukryte wydatki** – uważaj na ogłoszenia i reklamy obiecujące brak jakichkolwiek kosztów wstępnych a następnie zwracających się o jednorazową tylko opłatę.

UWAŻAJ TEŻ NA:

- łańcuszki listowe,

- listy wysyłkowe,
- domowe sieci handlowe,
- cudowne leki i środki upiększające,
- propozycje biznesowe z zagranicy.

PRZESTĘPSTWA KOMPUTEROWE (CYBERPRZESTĘPCZOŚĆ)

Przestępstwa internetowe w Polsce są jeszcze zjawiskiem rzadszym niż w USA czy Europie Zachodniej, ale zarówno kradzieże danych, jak i nielegalne transfery pieniędzy z kont osób fizycznych i podmiotów gospodarczych są notowane przez naszą policję.

Na całym świecie notuje się tygodniowo 33 mln ataków hakerów – wskazują najnowsze raporty dotyczące bezpieczeństwa w Internecie. Ciągle wzrasta liczba oszustw typu phishing: wyłudzanie, podszywanie się pod obce witryny, tworzenie fałszywych stron. Celem tych ataków jest wyłudzanie poufnych informacji, a szczególnie danych finansowych. Według *Anti-Phishing Working Group*, w samym tylko marcu 2005 r. odkryto ponad 2,8 takich fałszywych stron.

Coraz częściej przestępcy komputerowi zdalnie przejmują kontrolę nad komputerami. Mogą z nimi zrobić niemal wszystko: służą do rozsyłania spamu, przechowywania danych (np. nielegalnych kopii filmów) czy tzw. ataków DoS (Denial of Service) – blokowania witryn internetowych.

Natomiast dane dostarczone przez producenta oprogramowania antywirusowego McAfee sygnalizują nowe metody przejmowania kontroli nad nowoczesnymi modelami inteligentnych telefonów komórkowych. Napastnicy mogą bowiem uzyskać władzę nad telefonem poprzez protokół bezprzewodowy Bluetooth i wykorzystywać urządzenie do tych samych celów do których używane są komputery zombie PC.

Przestępstwa komputerowe, także te najpoważniejsze, są zjawiskiem, które występuje i to zagrożenie będzie się nasilało w miarę rozwoju Internetu. Zwalczanie przestępstw jest zadaniem policji. Przeciwdziałanie? Dużo zależy od samych użytkowników systemów informatycznych, tych którzy narażeni są na działania przestępców.

Każdy komputer podłączony do Internetu jest widoczny dla innych; identyfikowany przez adres IP. Nie oznacza to, że widoczne są wszystkie zgromadzone w nim informacje. O tym, jak konkretny komputer będzie widziany w sieci w tym, które z danych można zdalnie zmieniać, a które tylko przeglądać - może decydować jego główny użytkownik ustanawiając odpowiednie zabezpieczenia.

Jak dowodzi życie, wcale nie jest tak bardzo oczywistym fakt, że użytkownicy systemów komputerowych powinni być świadomi niebezpieczeństwa i robić wszystko, aby nie ułatwiać

przestępstw. Opacznie pojmowana oszczędność, niestosowanie się do zalecanych standardów bezpieczeństwa, niewykorzystywanie istniejących technik zabezpieczeń – to niektóre z dłuższej listy czynników, które mają wpływ na skalę przestępstw komputerowych. Trudno je wyeliminować, można je jednak ograniczać.

Użytkownicy systemów informatycznych i Internetu w Polsce narażeni są na podobne przestępstwa jak w innych krajach - nawet na sabotaż komputerowy, ataki z zagranicy itd. Zagrożenie, jakim są przestępstwa komputerowe zostało skatalogowane, co ma ułatwić ich zwalczanie. Zrobił to Komitet Ekspertów ds. Przestępstw Komputerowych Rady Europy. Do najpoważniejszych zaliczył ok. 10 rodzajów przestępstw, które nie są rzadkością także w Polsce.

Poważne w skutkach są ***oszustwa komputerowe***, których celem jest nieuprawnione zdobycie środków finansowych, zaś przedmiotem ataku: informatyczne systemy bankowe i finansowo-księgowe. Te przestępstwa trudno jest ścigać, gdyż poszkodowani nie są zainteresowani ujawnieniem słabości własnych systemów, aby nie utracić zaufania klientów.

Kolejny rodzaj to ***fałszerstwa*** tradycyjnych papierowych dokumentów przy użyciu komputera (i urządzeń peryferyjnych) oraz dokumentów elektronicznych przez wprowadzanie w nich zmian. Wykrycie tych przestępstw jest utrudnione, ponieważ zmiany dokonane przy wykorzystaniu nowoczesnych technologii niełatwo zauważyć.

Najczęściej występującym przestępstwem są ***włamania do systemów po pokonaniu zabezpieczeń (hacking)***. Polska policja ujawniała m. in. sprawców wielu prób i udanych włamań zgłaszanych przez administratorów sieci w kraju, a także próby włamań do systemów w Polsce dokonywanych np. z USA i innych krajów.

Niszczenie danych lub programów to przestępstwa, w których wykorzystywane są destrukcyjne programy – wirusy, konie trojańskie, bomby logiczne, robaki komputerowe. Dla użytkowników komputerów różnice między nimi mogą nie mieć znaczenia, ale dla ścigających są istotne. W przypadku bomby logicznej lub konia trojańskiego sprawcy należy szukać wśród osób uprawnionych do dokonywania zmian w oprogramowaniu natomiast krąg sprawców wprowadzenie wirusa lub robaka może być praktycznie nieograniczony.

Sabotaż komputerowy – kolejna kategoria. W Polsce takie sytuacje zdarzały się w związku ze zwolnieniami z pracy administratorów zakładowych sieci.

Poważnym zagrożeniem jest ***podsłuch komputerowy*** – przejmowanie informacji z transmisji danych lub przez analizę fal elektromagnetycznych.

Nasila się aktywność tzw. ***botnetów i komputerów zombie*** – zdalnie kontrolowanych sieci ubezwłasnowolnionych komputerów. Coraz częściej używane są one do kradzieży tożsamości i poufnych danych oraz dystrybucji i instalacji oprogramowania szpiegującego spyware. Według

szacunków *Honeynet Project*, co najmniej 1 milion komputerów na całym świecie jest zainfekowanych ukrytym oprogramowaniem umożliwiającym zdalną kontrolę. Typowy bonet może się składać średnio z 10 tysięcy komputerów, zarządzanych za pomocą systemu czatów IRC.

Botnety wykorzystywane są m.in. do blokowania serwisów firm świadczących usługi w sieci albo przejmowania kontroli nad domowymi lub firmowymi komputerami w celu uzyskiwania m.in. dostępu do historii operacji bankowych i innych poufnych danych użytkowników.

Powagę problemu może ilustrować sytuacja, kiedy zaledwie 6 zarażonych maszyn typu zombie było w stanie sparaliżować w kwietniu 2005 r. sieć największego australijskiego dostawcy Internetu, firmę BigPond.

Trwa nieustanny wyścig między tymi, którzy próbują "łamać" systemy komputerowe i systemy zabezpieczeń a ich twórcami. Jednak problem nie tyle w tym, kto ma przewagę - bo zdarzają się "genialni hakerzy", ale nie brakuje także równie sprawnych intelektualnie twórców zabezpieczeń. Problem leży w wykorzystaniu istniejących możliwości technicznych i przestrzeganiu obowiązujących standardów bezpieczeństwa.

- **Zdecydowałem się zawiadomić Policję o włamaniu do mojego komputera, jakie w związku z tym powinienem podjąć działania i jakie są wymagania formalne wniosku?**

Ustawodawca ustanowił hacking przestępstwem ściganym na wniosek poszkodowanego. Oznacza to, że procedura ścigania rozpoczyna się po złożeniu przez pokrzywdzonego wniosku o ściganie. Wniosek ten może być składany ustnie do protokołu podczas osobistego stawienia się w jednostce policji albo jednostce prokuratury właściwych dla miejsca popełnienia przestępstwa.

- **Ujawnianie ważnych danych w sieciach Peer-To-Peer**

Dość często zdarzają się przypadki nieświadomego ujawniania przez użytkowników Internetu swoich danych rejestracyjnych w sieciach P2P (np. eDonkey, iMesh, Kaaza). Upublicznienie tych danych następuje w wyniku udostępnienia dysku komputera lub katalogu, a w nich pliku zawierającego dane rejestracyjne. Dane rejestracyjne użytkownika (tj, dane osobowe, login, hasło, ID i PIN) powinny podlegać szczególnej ochronie, gdyż ujawnione nieuprawnionym osobom, mogą być wykorzystywane na przykład do popełnienia przez nich przestępstwa. Użytkownicy oprogramowania P2P powinni pamiętać, że udostępnienie dysku lub zawartości katalogu powoduje, iż wszystkie podkatalogi i wszystkie piki w nich umieszczone są widoczne dla innych użytkowników sieci.

NA CO UWAŻAĆ W UMOWACH Z DOSTAWCAMI USŁUG INTERNETOWYCH?

Wraz ze wzrastającą popularnością usług internetowych, coraz bogatsza staje się oferta firm świadczących usługi dostępu do Internetu. Okazuje się jednak, że dostawcy usług internetowych nie zawsze chcą odpowiadać za jakość dostępu do sieci albo nie zwracają abonamentu za przerwy w świadczeniu usług. Coraz częściej też określone postanowienia umów z dostawcami usług internetowych uznawane są przez sądy ze niedozwolone postanowienia umowne (zakazane klauzule).

W umowie z dostawcą Internetu należy zatem sprawdzić:

- czy dostawca nie odłącza automatycznie dostępu do sieci w razie krótkiego opóźnienia w płatnościach,
- czy nie nałożono obowiązku uiszczania opłat nawet wówczas, gdy nie otrzymujemy faktury,
- czy operator nie wyłącza swojej odpowiedzialności za nieprawidłowe działanie Internetu,
- czy nie trzeba płacić abonamentu w razie przerw w dostępie do sieci,
- czy przedsiębiorca nie zastrzegł wygórowanych kar umownych za opóźnienia w zapłacie.

Niedopuszczalne jest zastrzeganie w umowach, że klient ma obowiązek zapłaty abonamentu także wówczas, gdy nie otrzyma faktury lub książeczki opłat. W takich sytuacjach użytkownik powinien niezwłocznie poinformować operatora o braku faktury i czekać na jej dostarczanie. Za opóźnienie spowodowane niedostarczeniem faktury w terminie operator nie ma prawa naliczać odsetek za zwłokę.

W innych sytuacjach opóźnienia się przez abonenta z płatnością rachunku, operator może żądać odsetek za czas opóźnienia. Może również wyznaczyć dłużnikowi odpowiedni termin do uregulowania zobowiązań, z zastrzeżeniem, że jeśli tego nie zrobi, umowa zostanie rozwiązana. Bezprawne są natomiast praktyki firm polegające na automatycznym wyłączaniu usług w razie opóźnienia wynoszącego kilka dni, a następnie uzależnianiu ponownej aktywacji od zapłaty, często bardzo wysokiej opłaty manipulacyjnej.

Zdarza się również, że operatorzy zastrzegają w regulaminie świadczenia usług, że mimo przerwania świadczenia usług bądź ich zawieszania lub ograniczenia, naliczana jest pełna opłata za Internet. Klient płaci wówczas abonament nie otrzymując żadnego świadczenia lub otrzymując je w ograniczonym zakresie. W takich sytuacjach pamiętajmy, że za każdy dzień przerwy w świadczeniu usługi przysługuje nam prawo odliczenia odpowiedniej części opłaty, czyli zwrot 1/30 miesięcznej opłaty abonamentowej w drodze złożenia standardowej reklamacji.

Niektóre firmy zastrzegają, że abonent nie ma prawa wnosić żadnych roszczeń do operatora związanych z brakiem dostępu do Internetu, spowodowanym trudnościami technicznymi. Inne firmy wyłączają odpowiedzialność za szkody związane z utratą lub opóźnionym przesyłem danych czy nieprawidłowym działaniem sieci. Tymczasem każde roszczenie klienta o naprawienie szkody powinno być rozpatrywane indywidualnie zgodnie z ogólnymi zasadami prawa cywilnego.

W sytuacjach, gdy podpisaliśmy z tą samą firmą dwie umowy, jedną na usługi telefoniczne, druga – na usługi internetowe (np. w TP S.A. tradycyjna umowa o świadczenie usług telefonicznych oraz umowa o świadczenie Neostrady tp), niedopuszczalne są działania operatora polegające na odłączaniu linii telefonicznej w sytuacji gdy reklamujemy rachunek za usługi internetowe lub opóźniamy się z płatnością za te usługi. Są to dwie odrębne umowy, a operator nie może dowolnie przerzucać skutków wynikających z umowy o usługi internetowe na świadczenie usług telefonicznych.

SŁOWNICZEK

Netykieta – zespół zasad i norm dobrych obyczajów panujących w Internecie, czyli swojego rodzaju „konstytucja" zasad dobrego wychowania użytkowników Internetu.

Phishing – podszywanie się pod strony firm, najczęściej banków, i wyłudzanie zastrzeżonych czy też poufnych danych, np. numerów kart kredytowych, numerów rachunków bankowych, haseł, PIN-ów.

Spyware (oprogramowanie szpiegujące) – każde oprogramowanie, które zbiera informacje o użytkowniku i jest zainstalowane bez jego powiadomienia lub kontroli.